The SR 11-7 Blind Spot: What Banks Discover When AI Hits Model Risk Management

Your Model Inventory Has a Gap Your Regulators Are About to Find.

01

Background

How the 2011 model risk framework is now governing your 2025 AI deployments.

01 — BACKGROUND

SR 11-7 was written for logistic regression. You are running it on GPT.

- SR 11-7, issued by the OCC and Federal Reserve in 2011, governs model inventories, validation requirements, and governance processes at U.S. banks. It was written for statistical risk models — credit scoring, VaR, stress testing, prepayment models.
- Banks have deployed AI at scale: JPMorgan's contract analysis AI (COiN) and LOXM trading system, Wells Fargo's Fargo assistant, Bank of America's Erica (2B+ interactions). Regional banks are deploying third-party AI tools for credit, BSA/AML, and compliance monitoring.
- OCC (2021, 2023), Federal Reserve (2023), and FDIC (2023) have each issued guidance indicating AI/ML is subject to SR 11-7. None specify how to apply validation requirements to third-party LLM APIs whose internals are not disclosed.
- SR 11-7 validation assumes you can inspect the model, run it independently, and test challenger models. For a third-party LLM API, the model is a black box over HTTPS. The bank cannot validate what it cannot inspect.
- Examination teams are beginning to incorporate AI governance questions into standard safety and soundness exams. Banks without model inventory coverage for AI tools are building findings.

02

Decision Required

The question in front of every bank's model risk management team right now.

02 — DECISION REQUIRED

Is your AI tool a 'model' under SR 11-7 — and if it is, can you actually validate it?

SR 11-7 defines a model as a quantitative method or system that applies statistical, economic, or mathematical theories to data inputs, producing outputs used for decision-making. Most bank legal teams have concluded that AI tools in credit, fraud, compliance, and customer operations meet this definition.

If in scope: model inventory entry, validation plan, documented performance standards, ongoing monitoring, and model change governance are all required. For third-party LLM APIs, each of these obligations has an implementation gap.

Model changes are the acute risk. When OpenAI updates GPT-4 to GPT-4o, behavior changes materially. SR 11-7 requires impact assessment before model changes affect consequential outputs. Banks running third-party AI APIs are not in the change management loop.

03 — OPTIONS

Four governance postures on AI and SR 11-7.

Option A

Treat AI as tools — no inventory entry

Argue AI tools in advisory or assist roles do not meet the model definition. Viable for narrow use cases (internal doc summarization). High examiner risk if tool is in credit, fraud, compliance, or customer-facing workflows.

Option B

Recommended

Inventory all AI, validate to the extent possible, document gaps

Add all in-scope AI to model inventory. For third-party APIs, conduct output testing, adversarial testing, and demographic parity analysis. Document validation limitations explicitly. Establish model change monitoring. This is the defensible posture under current guidance.

Option C

Restrict AI to non-consequential use cases only

Limit AI to internal productivity tools that do not touch credit, fraud, compliance, or customer decisions. Eliminates SR 11-7 model inventory risk. Forfeits competitive advantage where AI ROI is highest. Not a sustainable long-term posture.

Option D

Self-hosted models only — full internal validation

Require bank-controlled infrastructure for any inventoried AI model. Eliminates third-party API black-box risk. Realistic only for top-20 banks by assets with ML engineering capacity. Most regional and community banks cannot execute this posture.

04 — RECOMMENDATION

Build the model inventory before the examination — not during it.

Audit every AI tool in use across the bank, including business unit and departmental shadow deployments not in formal technology acquisition records.

Apply the SR 11-7 model definition test to each tool with written documentation of the reasoning — not just the conclusion. Ambiguous cases should err toward inclusion.

For third-party API models, build a validation protocol around what is testable: output performance testing, adversarial scenario testing, demographic parity analysis for credit tools. Document the validation gap explicitly in the model file.

Establish a model change monitoring process: subscribe to provider release notes, designate a model owner, define the threshold that triggers formal re-validation.

Align with internal audit now. Model risk governance is an audit-covered domain. AI tools in scope for SR 11-7 without inventory entries appear in internal audit findings first.

Brief your primary regulator proactively if you have consequential AI deployments. Every OCC district office prefers a pre-exam briefing over discovering undisclosed model risk in examination.

05 — RISKS

Five risks that turn examiner observations into findings.

1.

Undisclosed model inventory gaps

An AI tool in credit decisioning, fraud detection, or compliance monitoring that is not in the model inventory is an SR 11-7 finding. The finding does not depend on whether the tool performed correctly — it depends on whether your governance process covered it.

2.

Unmanaged model version changes

Third-party AI providers update models without prior notice. Each GPT or Gemini version change that occurs without triggering an impact assessment is an undocumented model change event in your inventory record. Most bank governance processes were designed to catch internal model retrains, not API provider updates.

3.

Fair lending exposure in AI-assisted credit

AI tools in credit underwriting, pricing, or marketing require disparate impact analysis. Most banks that deployed AI credit tools in 2023–2024 have not completed this analysis for current model versions in production. The compliance gap compounds with each untracked version update.

4.

Vendor concentration risk across the inventory

Banks deploying multiple AI workflows on a single provider (OpenAI, Azure AI, Vertex) have created a single dependency spanning multiple model inventory entries. A pricing change, outage, or API deprecation affects multiple critical workflows simultaneously.

5.

Model validation team capability gap

Teams built for statistical model validation do not have the tools or methodology to validate LLMs. Validation reports that satisfy procedural requirements but miss LLM-specific failure modes (hallucination, prompt injection, context sensitivity) create an inadequate validation methodology finding even when validation is technically performed.

06 — QUESTIONS

Six questions your model risk committee should answer today.

1. Do you have a complete inventory of every AI tool in use at your institution, including deployments procured through business unit budgets or SaaS subscriptions outside formal model risk governance?
2. Has the SR 11-7 model definition test been applied to each AI tool, with written documentation of the reasoning for inclusions and exclusions?
3. For third-party LLM APIs in your inventory: what validation has been completed, what limitations are documented, and who is the designated model owner?
4. What is your process for detecting and assessing model version changes from third-party AI providers — and who is responsible for triggering re-validation?
5. Has a fair lending disparate impact analysis been completed for every AI tool in credit decisioning, pricing, or customer communication affecting account status?
6. When did your primary regulator last receive a briefing on your AI governance posture — and has your AI inventory grown materially since that briefing?

AI INSIGHT LAB

The Deployment Memo

One enterprise AI deployment, dissected every Tuesday.
Written for executives who have to decide, not just read.

Subscribe at aiinsightlab.cloud — free during beta.